UNITED STATES MARINE CORPS
MARINE CORPS LOGISTICS BASES
814 RADFORD BOULEVARD
ALBANY, GEORGIA 31704-0323

IN REPLY REFER TO:
2000
G600
JUN 1 0 2002

POLICY STATEMENT 12-02

From: Commander
To: Distribution List

Subj: SMALL SYSTEMS SECURITY POLICY

Ref: (a) IRM 5239-10 Small Computer Systems Security
(b) MARADMIN 162-00 Information Assurance Bulletin 2-00, Appropriate Use of Government Information Technology (IT) Resources
(c) MARCORLOGBASES Computer Software Policy
(d) MCO P5510.18 U. S. Marine Corps Information and Personnel Security Program Manual
(e) MARADMIN 375-01 Interim Policy on Appropriate Use of Personal Electronic Devices
(f) MARADMIN 541-99 Information Assurance Bulletin 2-99, Guidance on the Use of Commercial Electronic Mail (Email) Services

1. Purpose. The purpose of this policy is to establish guidelines and to inform the end-user of their responsibilities in regard to small systems security.

2. Background. The individual user is the first line of defense for protection of a computer theft or unauthorized access. The responsible individual should consider all aspects of security for their computer including, data security, physical security, and software security. Reference (a) offers specific guidance.

3. Policy. Federal Government communication systems and equipment (including Government owned and leased telephones, facsimile machines, electronic mail, internet systems, and commercial systems when use is paid for by the Federal Government) shall be for official use and authorized purposes only in accordance with reference (b). This policy defines the roles and responsibilities for personnel in paragraph 6 of this document. Supervisors will ensure their personnel are aware and understand their responsibilities and liabilities. Additional restrictive guidance may be implemented, based upon local requirements.

a. Data Security. The individual user is responsible for safeguarding the data on their computer. Users and administrators will ensure that certain protection measures are considered concerning data security.

(1) Properly store media storage devices, i.e., disks and removable hard drives.

(2) Secure original documents at the close of business.

(3) Make backups of hard drives if needed.

(4) Use a screen saver with a password on all operating systems, configured between 1 and 15 minutes, to ensure additional protection.

(5) Keyboard-lock the workstation, if possible, when leaving the desk for brief periods of time and completely power off the computer at the end of the workday.

(6) Memorize passwords and do not write them down on an unsecured piece of paper or store on the person.

(7) Certain passwords will be written down and placed in a sealed envelope and secured in a vault or container in order to retrieve them in unforeseen circumstances when no one with the password knowledge is available, i.e. router and all system administrator passwords.

(8) The virus protection procedures will be followed:

(a) The most recent Marine Corps version of antivirus software will be loaded to the system.

(b) All viruses will be reported to the appropriate Information Systems Coordinator (ISC) in order for it to be officially reported to higher headquarters.

(c) Good diskette controls such as scanning disks before opening any files on them will be used.

(d) Antivirus software definition files will be updated on a regular basis. Contact the ISC for questions concerning this process.

(e) All hard drive files will be scanned at least once a week.

(f) Caution will be used when opening e-mail attachments, as they may be infected. If there is any doubt about an attachment, call your ISSO for guidance.

(9) Attend annual computer security awareness training, as mandated by Public Law 100-235.

b. Physical Security. The physical access control measures are one of the best methods for denying unauthorized access. Ensure that the following measures involving physical security are taken into consideration.

(1) Post access rosters of approved individuals if necessary.

(2) Secure windows and doors when vacating office spaces.

(3) Maintain accurate inventories of computer equipment and software.

(4) Use surge protectors to help protect the system from power spikes.

c. Software Security.

(1) Game software is only authorized if it comes with a new machine or if it is an authorized military game. New machines that come with solitaire or other games, which are not removed by the local IT support section when issued, may be played during non-working hours such as lunch. Additionally, a new concept involving improving the military's warfighting skills using computer-based wargames is authorized during working hours if the supervisor permits.

(2) Secure all software packages in an area that will allow accountability of the software at all times. Keep the reading material and media together if possible.

(3) Some software used on government machines may also be used in the home to perform duties relating to the governmental work duties. It is important to check with the licensing agreements for verification. Reference (c) provides detailed guidance.

d. Classified information. The introduction of classified information onto a computer involves specific steps that must be followed. Reference (d) provides additional guidance.

(1) Attend the necessary security briefs associated with the data classification.

(2) Contact the local Base Security Manager or Information Systems Security Manager (ISSM) if the requirement exists to access/process/view classified information on a portable computer that is not permanently located in a secure area.

(3) Immediately report to the activity security manager if classified information is inadvertently generated/stored on a system outside of a secure space. The compromise of classified information can present a threat to the national security. Once a compromise is known to have occurred, the seriousness of damage to U.S. interests must be determined and appropriate measures taken to negate or minimize the adverse effect of such compromise.

(4) Affix colored security labels indicating the level of security to removable hard drives or any storage device containing classified information.

(5) Store portable media (i.e. floppy disks, backup tapes, etc.) in a properly approved container as to the classification of information on the media.

e. Portable computers or devices. These systems include notebooks and laptops.

(1) A portable computer and/or any peripheral devices (such as modems, fortezza cards, portable printer devices, etc.) used for a temporary additional duty (TAD) trip will not be left unattended.

(2) Portable computers used in or near controlled work areas will have all audio and video recording features properly disabled. Connectivity of a portable computer to a classified information system is prohibited unless approved by the Local Base Security Manager and the ISSM.

(3) Portable computer devices that have been connected to the SIPRNET will be stored in an approved storage container when not under direct surveillance.

(4) All portable computers will be used for Official Use and Authorized Use only.

f. Personal Electronic Devices (PEDs). PEDs include Personal Digital Assistants (PDAs), Palmtops, hand-held computers, cellular telephones, two-way pagers, wireless e-mail devices, and audio and video recording devices.

(1) Reference (e) discusses the use of these devices, including classified use, removable storage media, removable peripheral/expansion devices, audio recording capability, software, network connection and the physical security use. Reference (e) will be used to in all cases concerning government, contractor- or individual-owned PEDs.

(2) Only government-owned-and-issued devices are authorized to connect to the Marine Corps Enterprise Network (MCEN) (i.e. contractor and individually owned are not authorized).

(3) Government-owned PEDs will not be connected at any time to personally-owned computer equipment (i.e. 'hotdocking' between government and non-government owned computers).

(4) PEDs are not authorized in areas where the primary type of data being processed, stored or discussed is classified.

(5) Use of PED modems while the device is connected to a networked computer is unauthorized as this could create a 'backdoor' to the MCEN.

(6) Use only software from the approved software list and download, if necessary, only from an authorized site.

(7) Users must expect that any information stored on a PED will be subject to exposure.

(8) Use of commercial e-mail services such as palm.net is prohibited.

(9) Physically secure the PED and the cradle when not in use in order to prevent unauthorized users from hot-synching.

(10) Ensure that these devices are added to the appropriate Responsible Officer (RO) account and are assigned to an individual by name and organization.

g. Personnel security. People are the most serious threat to the security of a computer. All areas should be considered when planning for this threat. Disgruntled individuals internal to the organization could definitely be reason for concern.

(1) Attendance by MARCORLOGBASES computer users of the regularly scheduled Information Assurance awareness training is mandatory.

(2) Delete and remove access to accounts (mainframe, network, administrative rights to PCs, etc.) for civilian, military, or contractor personnel upon leaving the base permanently.

(3) Publicize procedures to report security violations and irregularities if necessary.

(4) Encourage personnel to be involved in contingency planning and risk analysis.

(5) Maintain awareness to unusual or stressful employee behavior, i.e., low morale, refusal to take leave, or personal problems. These may indicate vulnerabilities which could lead to an information security breach.

(6) Stress importance of personal integrity and ethics, and encourage the reporting of suspected security violations.

(7) Grant the minimum required access to data and directories for authorized personnel on a need-to-know basis.

h. Privately owned computers or devices. These are computers or devices that belong to individuals, not the Government. They will not normally be brought to the work area. Doing so can create a mistaken assumption that the data on that computer is still the owner's when in fact any newly added information would belong to the Government.

(1) Protect data that is taken home via removable media (floppy, zip, jazz, etc.) by using the governmental standard of virus protection, available for home use to all active government DoD employees to include military and civilian personnel.

(2) Ensure that malicious code is not downloaded to the privately owned computer if visiting web sites while interacting with governmental data. This could affect the integrity of the data.

(3) Governmental data will not normally be sent to a commercial Internet service provider (ISP) account, per reference (f).

4. Administrative Actions. Failure to abide by this policy will result in administrative or punitive action. This may include loss of account access.

5. Point of Contact. Address questions concerning Information Assurance to MARCORLOGBASES AC/S, Information Technology Department, Information Assurance Office (G620) at DSN 567-7133 or Commercial (229)-639-7133. Email is matcomg6iaoffice@matcom.usmc.mil. Information can also be obtained from the MARCORLOGBASES G6 Information Assurance Office website at http://www.ala.usmc.mil/iao.

6. Applicability. This policy is applicable throughout all activities aboard MCLB Albany, MCLB Barstow, and Blount Island Command.

R.S. Kramlich
R. S. KRAMLICH

Distribution: A

Mc-Alb5001/2(10-2001)
Inter-Department Route Sheet
CHIEF OF STAFF

Date 21 May 2002

File Name

2000/G600

SUBJECT

Policy Statement 12-02
Small Systems Secu;rity Policy

OPERATING CODES

M-- Originating or Office Affixing Route Sheet
A-- Appropriate Action
B-- Guidance
C--Signature
D--Comments
E--Recommendation
F-- Concurrence

G--Information
N--Return to ____________
I-- Initial
J-- Disposition
K--Decision
L-- Retention
O--Other______________

Nature Of Action	Originator's Initial	Due Date If Any
Routine		
Urgent		

Reference Held By (Name,Grade,Telephone,Office Code)

Routing : Use numbers to show order of routing

RTG CODE	RTG CODE	ADDRESSES	IN	OUT	Concur	NON Concur	INITIAL
	C	COMMANDER MARCORLOG BASES (L01)		5/22	RSK		
		CHIEF OF STAFF (L02)					
		DEPUTY CHIEF OF STAFF (L02)					
		STAFF SECRETARY (L03)					
		SERGENT MAJOR (L04)					
		BLOUNT ISLAND (90)					
		MCLB ALBANY (A01)					
		MCLB BARSTOW (B100)					
		MAINTENANCE CENTER ALBANY (880)					
		MAINTENANCE CENTER BARSTOW (B870)					
		LOGISTICS OPERATION CENTER (L10)					
		MAINTENANCE DIRECTORATE (L20)					
		SUPPLY CHAIN MANAGEMENT CENTER (55)					
		COMPTROLLER (40)					
		CONTRACTS (89)					
		STAFF JUDGE ADVOCATE (120)					
		MARCORLOGBASES INSPECTOR (L05)					
		BUSINESS OPPORTUNITY CENTER (L08)					
		COUNSEL (L06)					
		BASE ADJUTANT (A500)					
		INFORMATION TECHNOLOGY (G6)					
		MARKETING OFFICE (L30)					
		CIVILIAN HRO (L09)					

Remarks and Signature
If additional space is necessary use reverse

Kathy,
For Gen Kramlich's signature. POC is Valerie Byrd x6661 or Nancy Botwinick at x6025.

Please call when signed.

r/s
Nancy